Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
1/-The UDP protocol reveals that there is a problem retrieving the IP address of the website's domain name using the DNS protocol, as the UDP packet was undeliverable to port 53 of the DNS server. Specifically, the UDP message requesting the IP address for the domain of the website was not reachable at port 53 of the DNS server. 2/-This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDPport 53 unreachable 3/-The port noted in the error message is used for: connection between my computer and the DNS server 4/-The most likely issue is: In the DNS server is not responding because of the error found in the 53 port

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
1/-Time incident occurred: at 1:24 pm 2/-Explain how the IT team became aware of the incident: Several important clients reported that they were unable to access the website services and encountered an error message: 3/-Explain the actions taken by the IT department to investigate the incident: **Actions Taken:** The cybersecurity analysts were called to write a detailed report on the incident. The issue will be handled by a group of engineers who are working to resolve the problem by: 1. Using analysis tools in a Unix system, like Tcpdump, to analyze data packets. 2. Converting the data packets into datagrams for logging and further analysis. 3. Investigating whether the issue lies with the protocol type, port number, server, or

devices.

4. Assessing if there is a malicious attack or if there is an absence of critical security tools, such as a firewall

4/-Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
53 port Of the DNS server , the UDP packet and the ICMP error protocol

5/-Note a likely cause of the incident:
I believe the problem lies with port 53, where access is being blocked. This could be due to DNS attacks, such as DDoS, or the overwhelming size of the requests in the UDP messages. Additionally, the issue might stem from the misconfiguration of either port 53 of the server, the DNS server in general, or the firewall. As a result, the DNS protocol is not functioning as expected. Each report indicates that the initial UDP packet is sent correctly from the source (computer) to the destination (DNS server), and the IP address of the DNS server is obtained without any issues. However, the problem arises in the response: the UDP packet requesting the IP address for the website domain cannot reach port 53 of the DNS server.